eurofins | Medical Device Testing



Cyber Security

Maximizing benefit by reducing risk.

Electronic medical devices and healthcare systems represent a growing risk to patients, hospitals and medical centers. The threat is not only to sensitive data, but to lives as well. Health care organizations have 300%-400% more medical equipment than other IT devices, and as a result, security and management can become overwhelming. Ensuring these devices are secured and managed properly is of critical importance.

Securing medical devices begins in the design phase and should be considered throughout the system development lifecycle. Ensuring proper controls are in place and identifying vulnerabilities should be central to the System Development Lifecycle methodology.

Eurofins Medical Device Testing has been a global leader in standards testing, QA testing, cybersecurity testing, and digital testing for decades. We use our expertise to help medical device manufacturers around the world secure products before, during, and after-market release.

Eurofins Medical Device Testing offers a full array of cyber security services to ensure medical devices meet the highest standards for security and align our testing with UL2900, which is recognized by international bodies as a sound security standard for medical and other connected devices.

By partnering with Eurofins Medical Device Testing and leveraging our world-class security testing services, you will greatly improve your product's security posture and ensure your customers and their patients are protected.

Choose Eurofins Medical Device Testing to help you:

- Secure designs and architectures.
- Provide adequate documentation and operational guides.
- Provide sufficient security controls.
- Ensure proper auditing, logging and alerting.

- Ensure application security.
- Validate security through penetration testing.

Whether you are in the design phase, or have had products in production for years, Eurofins Medical Device Testing can help secure and protect your medical devices to position you ahead of the competition.

Eurofins Medical Device Testing offers a full array of Security Assessment Services including comprehensive portfolio options to meet all your business security needs. These services are aimed at baselining your security posture and identifying vulnerabilities and threats. We take a risk-based approach considering likelihood of exploitation and business impact, so you can manage your remediation efforts in a way that aligns with your business priorities.

What do we assess for?

Eurofins Medical Device Testing will review your organization, systems, applications, and data for:

- Vulnerabilities
- Governance
  - Compliance
  - Configuration errors
  - Alignment with best practices
  - Management, monitoring, and policy enforcement
  - Encryption, authentication, and patching
  - Identity and access management

eurofins

Medical Device Testing



Our Risk Assessments are designed to meet your specific business needs. We customize each assessment to align with unique business, security, compliance and budgetary requirements. Our assessments can include any combination of the following phases, which can be combined for larger projects or delivered individually.

Testing Available

- **Governance Gap Assessment**
  - review of standards, policies, processes and all aspects of an organization's SDLC and security programs.
- **Compliance Gap Assessment**
  - A review of specific regulatory compliance requirements as they relate to device design and manufacturing.
- **Vulnerability Assessment**
  - A review of device security, with the goal of finding vulnerabilities and security weaknesses.
- **Web Application Security Assessment**
  - A review of device web applications with a focus on coding and configuration errors. Code review services to identify vulnerabilities and coding errors that leave the application susceptible to attack. A review of device web applications with a focus on coding and configuration errors. Code review services to identify vulnerabilities and coding errors that leave the application susceptible to attack.
- **Remote Security Assessment**
  - An assessment of all remote access mechanisms which are thoroughly reviewed for vulnerabilities, best practices, encryption, authentication, monitoring, design and management.
- **Penetration Testing**
  - Exploitation of vulnerabilities found with escalation of privilege and lateral movement throughout the enterprise. This simulates a real-world attack and tests the efficacy of existing controls and exploitation of vulnerabilities.
- **Wireless Security Assessment**
  - A review of wireless architectures, configurations and controls. We will assess authentication, encryption, monitoring, configuration, management, and much more.